

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

Cryptography Research, Inc.,

NO. C 04-04143 JW

Plaintiff,

**FIRST CLAIM CONSTRUCTION
ORDER**

v.

Visa International Service Assoc., et al.,

Defendants.

I. INTRODUCTION

In this lawsuit, Plaintiff Cryptography Research, Inc. (CRI) contends that Defendant Visa International Service Association (Visa) infringes eight CRI patents involving devices and methods for the security of financial transactions being conducted using "smartcards." On November 8-9, 2005, the Court conducted claim construction proceedings. This Order sets forth the Court's construction of disputed words or phrases in U.S. Patent No. 6,327,661. Disputes with respect to related patents will be addressed in subsequent Orders.

II. FACTUAL BACKGROUND

"Smartcards" is a term that describes a credit card which looks like an ordinary credit card, but which contains a microprocessor. When the smartcard is used and the associated financial information is transmitted, the circuitry of the microprocessor performs cryptographic operations to secure the financial and identity information from external monitoring.

1 External monitoring of the microprocessor in order to learn otherwise secret information is
2 an "attack." Before the inventions which are disclosed in the patents, smartcard transactions were
3 subject to external attack because the microprocessor contained in the smartcard uses electrical
4 power to perform its cryptographic operations. These operations result in voltage changes and
5 electromagnetic radiation. The power consumption of the microprocessor during computations
6 could be monitored by measuring the flow of current into the chip, or the electromagnetic signals it
7 radiates, in a process known as "Simple Power Analysis." During this external monitoring process,
8 by combining thousands of power traces measured during different computations, far smaller data-
9 dependent power variations may be analyzed to learn otherwise secret financial information. This
10 process of externally monitoring and combining data-dependent power variations in order to
11 determine the secret key or other secret financial or identifying information is termed "Differential
12 Power Analysis" ("DPA").

13 Each of the eight U.S. Patents asserted by CRI describe inventions designed to secure the
14 microprocessor against external monitoring of its electrical properties. These eight patents are U.S.
15 Patent Nos. 6,327,661 (the '661 patent), 6,278,783 (the '783 patent), 6,298,442 (the '442 patent),
16 6,304,658 (the '658 patent), 6,381,699 (the '699 patent), 6,539,092 (the '092 patent), 6,510,518 (the
17 '518 patent), and 6,654,884 (the '884 patent). CRI alleges that certain claims of these patents are
18 infringed by Visa-branded Smartcards. The Court invited the parties to submit a list of claim terms
19 for which they desired a construction.

20 III. STANDARDS

21 Claim construction is purely a matter of law, to be decided exclusively by the court.
22 Markman v. Westview Instruments, Inc., 517 U.S. 370, 387 (1996). Claims are construed from the
23 perspective of a person of ordinary skill in the art at the time of the invention. Markman v.
24 Westview Instruments, Inc., 52 F.3d 967, 986 (Fed. Cir. 1995). To determine the meaning of the
25 claim terms, the court's primary focus should be on the intrinsic evidence, that is, the claims, the
26 specification, and, if in evidence, the prosecution history. Primos, Inc. v. Hunter's Specialties, Inc.,
27
28

451 F.3d 841, 847-48 (Fed. Cir. 2006). In assessing the intrinsic evidence, the court must look first to the words of the claims themselves. See Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996). These words are to be given their ordinary and customary meaning unless it is clear from the specification and prosecution history that the inventor used the term with a different meaning. Id. The claims should be interpreted consistently with the specification. See Renishaw PLC v. Marposs Societa' per Azioni, 158 F.3d 1243, 1250 (Fed. Cir. 1998).

Where intrinsic evidence alone resolves any ambiguity in a disputed claim term, it is improper to rely on evidence external to the patent and file history. Vitronics, 90 F.3d at 1583, 1585. However, extrinsic evidence may be considered where intrinsic evidence is insufficient to enable the court to construe disputed claim terms. Id. at 1585. Common sources of extrinsic evidence include expert testimony, inventor testimony, dictionaries, and technical treatises and articles. Id. at 1584.

IV. DISCUSSION

A. Claim 1 of the '661 Patent

The '661 patent discloses the use of unpredictable information to minimize leakage from smartcards and other cryptosystems. One approach disclosed by the '661 patent is the modification of computational processes in implementations of cryptographic algorithms to incorporate new random information so as to conceal within or among the random information the secret information that might be sought by an attacker. Other embodiments of the '661 patent include techniques to prevent the temporal correlation of specific operations, symmetric permutation blinding, and the introduction of entropy into the order of operations. Col. 1, l. 64 - Col. 2, l. 49. The Court will consider each Claim of the '661 Patent over which there is a dispute.

Claim 1 of the '661 patent provides:

1. A **cryptographic processing** device for securely performing a **cryptographic processing operation** including a sequence of instructions in a manner **resistant to** discovery of a secret by external monitoring, comprising:

(a) an input interface for receiving a quantity to be **cryptographically processed**, said quantity being representative of at least a portion of a message;

(b) a source of unpredictable information;

(c) a processor:

(i) connected to said input interface for receiving and **cryptographically processing** said quantity,

(ii) configured to use said unpredictable information to **conceal a correlation** between externally monitorable signals and said secret during said processing of said quantity by **modifying said sequence**; and

(d) an output interface for outputting said **cryptographically processed** quantity to a recipient thereof.

1. "cryptographic processing; cryptographic operation"

The parties dispute over the meaning of the phrase "cryptographic operation," which appears in various claims throughout the asserted patents. The dispute also encompasses the related terms "cryptographic processing operation," "cryptographic processing," and "cryptographically processed."

One aspect of the dispute is whether the phrase "cryptographic operation" should be limited to encryption and decryption.

The specification refers to "cryptographic operations" as including more than simply encryption and decryption. For example, in the '442 patent: "Such keys are used in connection with various cryptographic operations including, without limitation, symmetric encryption using DES, triple DES, IDEA, SEAL, and RC4; public key (asymmetric) encryption and decryption using, RSA and ElGamal; digital signatures using, DES, ElGamal, and RSA; and Diffie-Heilman key agreement protocols." Col. 1, ll. 27-33.

The language of certain dependent claims also supports a broader definition. In the '699 patent, for example, Claim 9 provides "The cryptographic token of claim 7, wherein said cryptographic operations include DSA signing operations." Col. 22, ll. 7-8. Similarly, Claim 20 of the '658 patent provides: "The method of claim 19 where said asymmetric cryptographic operation includes a digital signing operation." Col. 24, ll. 30-31. Thus, "cryptographic operation" includes digital signing and cryptographic hashing.

1 The Court construes the phrase "**cryptographic operation**" to mean: "**an operation within**
2 **a class of techniques or algorithms used to secure data and avoid digital identity**
3 **misrepresentations.**"

4 **2. "resistant to"**

5 The parties dispute over the meaning of the phrase "resistant to," which appears in
6 independent Claim 1 of the '661 Patent. It also appears in Claims 6, 9, 11, 15, 26, 27, and 29 of the
7 '661 Patent; Claims 22 and 28 of the '783 Patent; Claims 1, 13, 18, and 31 of the '442 Patent; Claim
8 39 of the '658 Patent; Claims 2, 11, and 31 of the '518 Patent; and Claim 1 of the '884 Patent.

9 The parties dispute whether "resistant to" refers to "reduce" or "significantly reduce."

10 The plain and ordinary meaning of "resistant to" suggests that construction of "resistant to"
11 as either "reduce" or "significantly reduce" would be improper. Unlike "reduce" which is used to
12 compare the level of an entity with that entity's previous level, "resistant to" ordinarily describes a
13 relationship between the entity and an external force. The written description of the invention
14 supports this distinction. "Reduction" in S/N ratio involves a lessening of the original quantum of
15 S/N ratio. See '661 patent, col. 4, ll. 1-5. On the other hand, "resistance," is referred to in relation to
16 an "attack," as in "enabling the construction of devices that are significantly more resistant to attack
17 than devices of similar cost and complexity." '661 patent, col. 14, ll. 6-10.

18 "Resistant to" is also used in the claims in a manner which is consistent with its plain and
19 ordinary use: "resistant to discovery," Claim 1, '661 patent, "resistant to external detection," Claim 1,
20 '442 patent, and "resistant to detection," Claim 13, '442 patent.

21 The intrinsic evidence does not disclose a particular quantum of resistance as necessary to a
22 definition of the phrase.

23 The Court construes "resistant to" to mean: "**less susceptible to external influence.**"

24 **3. "modifying said sequence"**

25 The dispute over the phrase "modifying said sequence" is whether it is limited to
26 randomization.

1 The plain and ordinary meaning of "modification" is not restricted to randomization.
2 Reading the claim language in light of the written description suggests that limiting modification to
3 randomization would be improper. The '661 patent discusses the use of random information to
4 "select between parallel code processes, such that the same cryptographic result will be produced
5 regardless of which code process is selected but where the parallel processes perform different
6 operations toward producing the result." Col. 10, ll. 32-36. Each of the two parallel processes has a
7 fixed, or non-random, sequence. While the data may be processed in random order, the sequence of
8 operations itself is not completely random. Also, the patent states: "Although the embodiments
9 differ in the details of their implementations, those skilled in the art will appreciate the fundamental
10 commonality in their essential operation—using randomness *or other sources of unpredictability*."
11 Col. 2, l. 66 - Col. 3, l. 7 (emphasis added). The intrinsic evidence indicates that a modification may
12 render the data unpredictable in a manner which does not require randomness. There is no
13 indication that a person of ordinary skill in the art would limit "modify" to "randomize."

14 The Court construes "**modifying said sequence**" to mean: "**changing the order of the**
15 **sequence.**"

16 **4. "to conceal a correlation"**

17 The dispute as to the phrase "to conceal a correlation" mirrors the disagreement between the
18 parties with regard to the terms "reduce," "restrict," and "inhibit." One party contends that "conceal
19 a correlation" means "concealing any relationship." Another party contends that the phrase means
20 "decorrelate."

21 The claimed methods of the '661 patent are designed only to reduce the signal to noise ratio
22 "thereby increasing the number of observations required by an attacker to compromise the key."
23 Col. 3, l. 67 - Col. 4, l. 1. As used in the written description, "conceal" does not refer to a complete
24 concealment: "This high-entropy permutation combines several previously-described aspects of the
25 present invention, including without limitation order randomization (thus being neither
26 input-ordered nor output-ordered) and blinding techniques (to *conceal further* the data being
27 permuted)." Col. 11, ll. 34-39.

The plain and ordinary meaning of "conceal" is more than *de minimus*. In discussing clock skipping, the '661 patent acknowledges: "Of course, small temporal alignment variations may not be able to conceal signal characteristics that are of large amplitude or of long duration." Col. 6, ll. 57-59.

Consistent with the stated purpose of the invention in using "leak minimization and obfuscation" as "useful for improving security," '661 patent, col. 14, ll. 6-9, the Court construes "conceal a correlation" to mean **"hiding a correlation, so as to render an attack impractical."**

B. Claim 6 of the '661 Patent

Claim 6 of the '661 patent provides:

A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising:

(a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message;

(b) a source of unpredictable information;

(c) a processor:

(i) connected to said input interface for receiving and cryptographically processing said quantity,

(ii) configured to use said unpredictable information to **conceal a correlation** between said microchip's power consumption and said processing of said quantity **by expending additional electricity** in said microchip during said processing; and

(d) an output interface for outputting said cryptographically processed quantity to a recipient thereof.

Claim 6 claims a device in which random amounts of additional power are consumed to mask the key-dependent power consumption. Col. 5, ll. 28-29. The Court has previously construed "conceal a correlation." The Court finds no need to further construe the disputed phrases of Claim 6 of the '661 Patent at this time.

C. Claim 11 of the '661 Patent

Claim 11 of the '661 patent provides:

11. A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external

measurement of said device's power consumption, comprising:

...

(d) **a noise production system** for introducing noise into said measurement of said power consumption.

1. "noise production system"

The parties dispute whether the "noise production system" would merely "reduce the amount of information useful to an attacker," or must "not reveal information that is correlated to the secret." Based on the effectiveness limitations already contained in the claim language and on the Court's construction of "resistant to," the Court declines to further construe this phrase.

D. Claim 15 of the '661 Patent

Claim 15 of the '661 patent provides:

A cryptographic processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring of said device's power consumption, comprising:

(a) an input/output interface for receiving data to be cryptographically processed, said data being representative of at least a portion of a message;

(b) an input interface for receiving an external clock signal;

(c) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation;

(d) a source of unpredictable information;

(e) **a clock decorrelator** coupled to said source of unpredictable information for generating an internal clock signal from said external clock signal using said unpredictable information, such that said internal clock signal **cannot be reliably predicted** from said external clock signal; and

(f) a processor:

(i) clocked by said internal clock signal,

(ii) configured to cryptographically processing said data, and

(iii) configured to output said cryptographically processed data using said input/output interface.

//

1 **1. "clock decorrelator"**

2 The parties disagree on the meaning of "clock decorrelator" and the construction of "cannot
3 be reliably predicted." The parties dispute whether clock decorrelation is limited to causing the
4 skipping of random clock cycles, or whether clock decorrelation is a broader term.

5 Dependent Claim 16 claims "the device of claim 15 wherein said clock decorrelator
6 comprises a clock skipping module which selects a subset of the cycle of said external clock signal
7 to use as said internal clock signal based on said unpredictable information." '661 patent, col. 16, ll.
8 39-43. The inclusion in Claim 16 indicates that the clock decorrelator, as referred to in Claim 15 is
9 not limited to the particular clock skipping module described in Claim 16. See Phillips v. AWH
10 Corp., 415 F.3d 1303, 1324 (Fed. Cir. 2005).

11 In describing clock skipping, the written description appears to equate clock skipping with
12 clock decorrelation: "[W]hat will be referred to herein as clock skipping (or clock decorrelation),"
13 '661 patent, col 6, l. 17. Cf. Novacor Chems., Inc. v. U.S., 171 F.3d 1376, 1381 (Fed. Cir. 1999)
14 (recognizing that "general principles of construction support the view that a parenthetical is the
15 definition of the term which it follows" in interpreting a United States Customs regulation). See
16 also, '661 patent, col. 5-10 ("Clock skipping involves decorrelating cryptographic operations from
17 the normal [external] clock cycles").

18 Whether referred to as "clock skipping" or "clock decorrelation," however, the specification
19 describes a technique not limited to literally "caus[ing] random clock cycles to be skipped" as Visa
20 proposes:

21 Within clock skipping module 240, random output 205 is used to select cycles of
22 clock signal 220 to skip in order to produce clock signal 260. Alternatively,
23 random output 205 can be used to select the closest corresponding cycles of clock
24 signal 220 to be used as clock signal 260, or random output 205 can even be used
25 as clock signal 260 itself. Still other approaches are possible, as will be
26 appreciated by those skilled in the art; the basic point being that clock signal 260
27 be (partially or wholly) decorrelated from external clock signal 220 via random
28 output.

'661 patent, col. 7, ll. 36-45; See also, '661 patent, col. 9, ll. 60-62 ("all of the foregoing paragraphs
describe various ways to generate a second, internal clock signal: via randomization, via a separate
clock, or via derivation from the external clock").

1 The Court construes "**clock decorrelator**" to mean "**a device that generates an internal**
2 **clock signal that varies in a randomized way.**"

3 **2. "cannot be reliably predicted"**

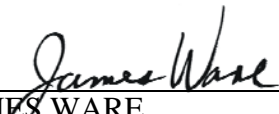
4 The parties dispute whether the phrase "cannot be reliably predicted" mean that there must
5 be perfect security.

6 The description of clock skipping and clock decorrelation in the specification also indicates
7 that "cannot be reliably predicted" is not limited to perfect security. The claim language "cannot be
8 reliably predicted" adequately reflects the variable effectiveness of the technique in different
9 situations, and thus, the Court declines to further construe the phrase.

10 **V. CONCLUSION**

11 Disputes with respect to related patents will be addressed in subsequent Orders. If a party
12 wishes further construction of the disputed phrases in the '661 Patent, a motion to that effect must be
13 made to the Court. The motion shall be filed pursuant to the Civil Local Rules of the Court.

14
15 Dated: October 19, 2006



JAMES WARE
United States District Judge

THIS IS TO CERTIFY THAT COPIES OF THIS ORDER HAVE BEEN DELIVERED TO:

Alexandra V. Percy apercy@hansonbridgett.com
Alka A. Patel patela@pepperlaw.com
Christopher J Huber huberc@pepperlaw.com
Darren E. Donnelly ddonnelly@fenwick.com
David Eiseman davideiseman@quinnemanuel.com
David Douglas Schumann dschumann@fenwick.com
David Douglas Schumann dschumann@fenwick.com
Erik N. Videlock videlocke@pepperlaw.com
J. David Hadden dhadden@fenwick.com
Jedediah Wakefield jwakefield@fenwick.com
Jedediah Wakefield jwakefield@fenwick.com
Kathryn M. Kenyon kenyonk@pepperlaw.com
Laurence Z Shiekman shiekmanl@pepperlaw.com
Laurie Michelle Charrington lcharrington@gmail.com
Lynn H. Pasahow lpasahow@fenwick.com
Marshall C. Wallace mwallace@reedsmith.com
Martin F. Majestic Mmajestic@hansonbridgett.com
Michael A. Duncheon mduncheon@hansonbridgett.com
Rachel Heather Smith rachelsmith@quinnemanuel.com
Roderick M. Thompson rthompson@fbm.com
Ryan Aftel Tyz rtyz@fenwick.com
Sangeetha M. Raghunathan sraghunathan@fbm.com
W. Joseph Melnik melnikj@pepperlaw.com
Willard R. Burns burnsw@pepperlaw.com
William Paul Schuck wps@mjllp.com

Dated: October 19, 2006

Richard W. Wieking, Clerk

By: /s/ JW Chambers
Elizabeth Garcia
Courtroom Deputy